PAT-NO: JP405314154A

DOCUMENT-IDENTIFIER: JP 05314154 A

TITLE: ELECTRONIC VOTING DEVICE

PUBN-DATE: November 26, 1993

INVENTOR-INFORMATION:
NAME
SAKO, KAZUE

ASSIGNEE-INFORMATION:
NAME COUNTRY
NEC CORP N/A

APPL-NO: JP04079745

APPL-DATE: April 1, 1992

INT-CL (IPC): G06F015/28

ABSTRACT:

PURPOSE: To prevent padded voting by taking one synchronization of all voters by adding an open phase instead of mutual certification.

CONSTITUTION: By a first voting phase, each voter 101(i) sends out an output s(i) to a center 100, respectively, and it is received by a primary voting sentence receiving means 206. Subsequently, by an open phase, the center 100 confirms whether or not the output s(i) is sent out surely by the voter 101(i) having the right of voting by a verifying means 203, and officially announces the output s(i) from the confirmed legal votor by a notice board 102. Also, for a primary voting sentence s(i) from the confirmed voter, a blind signature generator 204 outputs an integer (d) read out of a secret holding means 201 and

a fixed number holding means 202, and an output d(i) calculated by using a
verification fixed number (n), and a blind signature transmitting means 205
transmits this output d(i) to the voter 101(i). Subsequently, after secondary
voting, the center enumerates all votes sent in an unnamed state on the notice
board, and officially announces the total.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平5－314154

(43)公開日　平成５年(1993)11月26日

(51)Int.Cl.[5]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｇ０６Ｆ　15/28		Ｂ　7218－5Ｌ		

審査請求　未請求　請求項の数１(全　６　頁)

(21)出願番号　特願平4－79745

(22)出願日　平成４年(1992)４月１日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　佐古　和恵
東京都港区芝五丁目７番１号日本電気株式会社内

(74)代理人　弁理士　京本　直樹　（外２名）

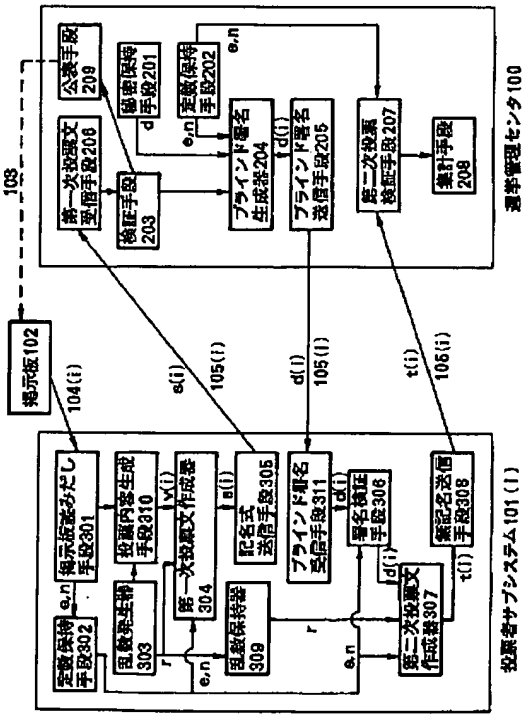
(54)【発明の名称】　電子投票装置

(57)【要約】

【目的】　電子的に無記名投票を行なうために、選挙管理センタによる結果判明後の水増し投票による投票結果操作を最小限におさえ、かつ投票者にとって負担とならない手間で実現する。

【構成】　投票を第一次投票フェーズと第二次投票フェーズにわけ、間に投票者数を公開する公開フェーズをいれる。

【効果】　公表フェーズをはさむことにより、選挙管理センタが投票結果を知る前に投票者の数が投票者に公表されるので選挙管理センタの水増し投票を防いでいる。また、投票者にとっては第一次投票フェーズから第二次投票フェーズへ移る同期を一度だけとればいいので、従来相互認証により２度同期をとっていた方式より手間が少なくて済む。



1

【特許請求の範囲】

【請求項1】　電子的に無記名投票を行なうために、あらかじめ定められた形式にしたがった投票内容を投票者が乱数を用いて変換したものを選挙管理者に送信する第一次投票手段と、選挙管理者が正当な投票者から送付された変換された投票内容に対して署名をし、それを投票者に返信する署名手段と、選挙管理者が第一次投票を行なった投票者の数を公表する公表手段と、各投票者が返信された署名文に対して、前記乱数を用いて、変換前の投票内容に対する署名文を作成し、署名付きの投票内容を無記名で送付する第二次投票手段と、正当な投票形式に正当な署名文が付加されていれば、投票結果を集計する集計手段とを有することを特徴とする電子投票装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は電子ネットワーク上で有権者だけが1度だけ無記名で投票できる電子投票装置に関する。

【0002】

【従来の技術】電子投票方法として従来から知られているものは太田の方法がある。これは特開平1－177164号公報及び昭和63年電子情報通信学会春季全国大会A－294「単一の選挙管理者を用いた電子投票形式」に開示されている。太田の無記名電子投票方式は、投票者が乱数を用いて変換した投票内容を投票者全員で相互認証したのち、選挙管理者に送信する第一次投票手段と、選挙管理者が正当な投票者から送付された変換された投票内容に対して署名をし、それを投票者に返信する署名手段と、各投票者が返信された署名文に対して、前記乱数を用いて、変換前の投票内容に対する署名文を作成し、投票内容と署名文を無記名で送付する第二次投票手段と、正当な投票形式に正当な署名文が付加されてあればその投票を集計する集計手段からなる。

【0003】

【発明が解決しようとする課題】太田の方法では選挙管理者による水増し投票を防ぐために、正当な投票者かどうかを相互認証で確認しているが、相互認証は投票者全員で同期を2度に渡ってとらなくてはいけないという問題がある。本発明の目的は、上述の欠点を除去し、選挙管理者による水増し投票を防ぐために、相互認証ではなく、公開フェーズを付加することにより、投票者全員の同期を一度とればよい電子投票装置を提供することにある。

【0004】

【課題を解決するための手段】本発明の電子投票装置は、あらかじめ定められた形式にしたがった投票内容を投票者が乱数を用いて変換したものを選挙管理者に送信する第一次投票手段と、選挙管理者が正当な投票者から送付された変換された投票内容に対して署名をし、それを投票者に返信する署名手段と、選挙管理者が第一次投票を行なった投票者の数を公表する公表手段と、各投票者が返信された署名文に対して、前記乱数を用いて、変換前の投票内容に対する署名文を作成し、署名付きの投票内容を無記名で送付する第二次投票手段と、正当な投票形式に正当な署名文が付加されていれば、投票結果を集計する集計手段とを有することを特徴とする。

2

【0005】

【実施例】次に、図1から図4を参照して本発明の実施例について説明する。

【0006】本発明の電子投票装置を、m個の投票者サブシステム101（1）～101（m）及び1つの選挙管理センタ100が相互に安全な通信チャネル（例えばデータ回線）105で結ばれており、さらに選挙管理センタ100のみが書き込み可能ですべての投票者サブシステムが読み出せる電子掲示板102が存在する無記名電子投票システム（図2）に適用する例を述べる。なお、以下簡単のために選挙管理センタをセンタ、投票者サブシステムを投票者と呼ぶことにする。

【0007】この投票システムは準備フェーズと、第一次投票フェーズ、公表フェーズ、第二次投票フェーズ及び結果公表フェーズからなる。本発明は第一次投票フェーズ、公表フェーズ、第二次投票フェーズに関する。

【0008】まず、図1と図3を用いて準備フェーズを説明する。

【0009】図1は、本発明の電子投票装置の一実施例を示すブロック図であり、図3は準備フェーズの一例である。

【0010】本無記名電子投票システムを実施するための準備として、センタ100は署名用の定数を設定し、検証用定数を電子掲示板102に掲示する。例えば、署名方式としてRSA暗号方式を用いるとする。そこで、nを二つの素数p，qの積とし、eとdをe・d＝1 mod（p－1）・（q－1）を満たす整数とする。このときセンタはe，nを検証用定数として設定し（ステップ11）、電子掲示板102に書き込む（ステップ12）。今後この検証用定数e，nは頻繁に用いられるので自分の定数保持手段201に書き込み容易にアクセスできるようにする（ステップ13）。一方、dは自分の秘密情報保持手段202に格納する（ステップ14）。

【0011】次に、センタ100は投票に関する規則を定める。まず、投票対象の議題を明らかにし、投票フォーマットを定める。たとえば、投票フォーマットは、上位第1ビットから第8ビットに選択肢番号を対応させ、第9ビットから、第128ビットに乱数を発生させ、次の64ビットは、第9ビットから第64ビットをDES暗号の鍵、第65ビットから第128ビットを平文とみなした場合の暗号文とするフォーマットとする（ステップ15）。

【0012】次に、投票する権利のあるサブシステム（以後、有権者と呼ぶ）の名前を一覧にする（ステップ

16）。第一次投票及び第二次投票の期限を設定・公表し（ステップ17）、第一次投票フェーズの開始を合図する（ステップ18）。

【0013】以上が準備フェーズである。

【0014】次に、第一次投票フェーズ、公表フェーズ、第二次投票フェーズを説明するが、各フェーズとも選挙管理センタ100は各投票者に対して同じ手順を踏むので、特定の投票者サブシステム101（i）に対する手順を例にとって説明を続ける。

【0015】図1に示すように無記名電子投票システムはセンタ100が電子掲示板102に定数及び投票規則を書き込む安全通信チャンネル103、投票者101（i）が電子掲示板102に書かれた内容を読み出すための安全通信チャンネル104（i）及び投票者とセンタが交信するための安全通信チャンネル105（i）で構成されている。

【0016】まず、図1を参照しながら投票者101（i）の第一次投票フェーズを説明する。

【0017】投票者101（i）は掲示板読み出し手段301を用いて掲示板102に書かれてある内容を読み出し、定数e，nを定数保持手段302に格納する一方、読み出したフォーマットに沿うよう投票内容作成手段310にて自分の意見に対応する投票内容v（i）を生成する。このとき、投票内容フォーマットが乱数成分を加味するのであれば、乱数発生器303の出力を用いる。次に、第一次投票文生成器304は、乱数発生器303の出力rと定数e，nを用いて、

$$s(i)=v(i)\cdot r^{e} \bmod n$$

を計算し、s（i）を出力する。また、このときの乱数発生器303の出力rは乱数保持器309に格納する。s（i）を記名付き送信手段305が安全チャンネル105（i）を通じてセンタ100に送信する。

【0018】以上が第一次投票フェーズであり、各投票者101（i）がそれぞれs（i）をセンタ100に送出する。センタ100はこれを第一次投票文受信手段206で受信する。

【0019】次に、公開フェーズでセンタは以下のことを行なう。

【0020】一つは、センタ100は第一次投票文受信手段206で受け取ったs（i）が確かに有権者である投票者101（i）が送出したものかどうかを検証手段203にて確認する。すなわち、チャンネル105（i）を通じて記名式で送られてきたものかどうかと、その名前が正当な有権者であるかどうかを確認する。確認できた正当な有権者からのs（i）を掲示板102にて公表する。

【0021】もう一つは、確認できた有権者からの第一次投票文s（i）に対して、ブラインド署名生成器204は秘密保持手段201、定数保持手段202から読みだしたd及びnを用いて、

$$d(i)=s(i)^{d} \bmod n$$

を計算し、出力する。ブラインド署名送信手段205はd（i）を投票者101（i）に送信する。

【0022】第一次投票を行なったすべての有権者に対してブラインド署名を送信すればセンタは第二次投票フェーズに移行することを宣言する。なお、この公開フェーズはすべての投票者が第一次投票フェーズを終了した時に行なってもよいし、あるいは第一次投票のために一定時間を設け、その期間が終了したら行なうことにしてもよいし、また、第一次投票を受信する毎に行なってもよい。

【0023】次に、第二投票フェーズを説明する。

【0024】署名検証手段306は、ブラインド署名受信手段311によりセンタ100から受信したd（i）と、定数保持手段302から読み出したe，nを用いて

$$s(i)=d(i)^{e} \bmod n$$

が成立するかどうか検証する。また、自分の第一次投票内容s（i）が掲示板に記載され、数えられていることを確認する。

【0025】確認できれば、第二次投票内容生成器307は、乱数保持器309から読みだした整数rと、定数保持手段302から読み出したnを用いて、

$$t(i)=d(i)/r \bmod n$$

を計算し、無記名送信手段308はt（i）を送信者名を付記せずにセンタ100に送出する。

【0026】センタ100は、第二次投票確認手段で、

$$t(i)^{e} \bmod n$$

を計算し、その出力、すなわち投票内容があらかじめ掲示板に記載されたフォーマットに従っているか否かを検証する。なお、この値は投票者が不正をしていなければ、v（i）に等しくなる。検証できれば、その投票内容を集計手段208で集計する。

【0027】全員の第二次投票が終了すれば、結果公表フェーズとして、センタは無記名で送付されたすべての投票を掲示板に列挙し、集計結果を公表する。各有権者は自分の投票が正しく記載されていることと、記載されている投票を集計すると確かに公表された集計結果になることを確認する。異議申し立てがなければ、この集計結果をもって、承認された投票結果とする。

【0028】図4を参照すると、このシステムは、通信処理機能を備えたパーソナルコンピュータ等の端末装置（TMU）401と、読み出し専用記憶装置（ROM）402と、ランダムアクセス記憶装置（RAM）403と、乱数発生器（RNG）404と、シグナルプロセッサ（SP）406と、TMU401、ROM402、RAM403、RNG404及びSP406を相互に接続する共通バス405とから構成される。

【0029】RNG404は乱数SP406の指令により発生する。これはセンタ100が定数設定の時に用い、また、各投票者101（i）の乱数発生器として用

5

いる。ROM407にはセンタ100の場合、定数e，nと秘密情報dを記憶している。dはTMUからブラインド署名作成の度にRAMに格納するようにしてもよい。ROM407には投票者サブシステム101（i）の場合、定数e，nを記憶している。ROM内に格納されたプログラムに基づいて、上述の動作を実現する。RAM403はこれらのステップの実行中に計算途中結果等を一時的に記憶するために用いられる。

【0030】また、システム100，101（i）は汎用電子計算機等のデータ処理装置やICカードであってもよい。

【0031】ここで、この方式が二重投票を防いだ無記名の電子投票システムになっていることを示す。

【0032】まず、無記名であることは第二次投票フェーズで無記名送信手段を用いるので、センタにはだれがどの投票内容を送ったが追跡できない。追跡できなければ、同じ人が何度も投票するかもしれない。しかし、そのためには第一次投票フェーズを投票回数分通過しないと第二次投票確認手段で通過するような投票内容を得られない。しかしながら、第一次投票フェーズは記名式で行なっているので、同一人物が2度以上実行することをセンタは検出できる。最後に、第一次投票フェーズを記名式で行なっても、第二次投票の無記名性が保たれるのは同一人物が送った第一次投票の内容と第二次投票の内容は送信者のみが知られている乱数により関係付けられているので、センタには関係がわからない。

【0033】しかし、従来の方式では、第一次投票フェーズと第二次投票フェーズの間に公表フェーズがなかったために、センタは以下のような悪事ができた。すなわち、公開フェーズがないために、投票者数を全員に知らせることなく集計結果をしることができた。したがって、センタの意にそぐわない集計結果になりそうな場合は、投票欠席者の代わりに自分の思い通りの投票で埋めることができる。

6

【0034】したがって、この悪事を防ぐために、投票者数を全員に知らしめるべく相互認証を用いた方式を採用していた。しかし、相互認証を用いた方式は各投票者同士でお互いを確認するので、2度にわたって全員で同期をとる必要があり、この方式を実装するには実用的ではなかった。

【0035】このような欠点は公表フェーズをとり入れた本発明で解決できる。すなわち、センタは集計結果を知る前に、投票者数を公表しなくてはならないので、欠席者の代わりに自分で投票を偽造しても検出される。また、第一次投票から第二次投票に移る際に一度だけ同期をとればいいので、実用的な方式である。

【0036】

【発明の効果】以上詳細に説明したように、本発明を用いれば、センタによる水増し投票を防いだ、実用的な無記名電子投票システムを構築できる。

【図面の簡単な説明】

【図1】本発明の電子投票装置の一実施例を示すブロック図。

【図2】無記名電子投票システムを示す図。

【図3】準備フェーズの例を示す図。

【図4】センタ100、投票者サブシステム101（i）の構成を示す図。

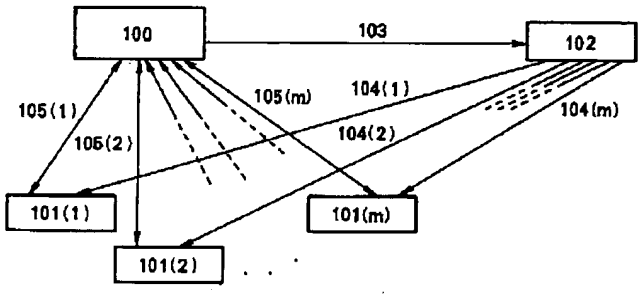
【符号の説明】

100　選挙管理センタ

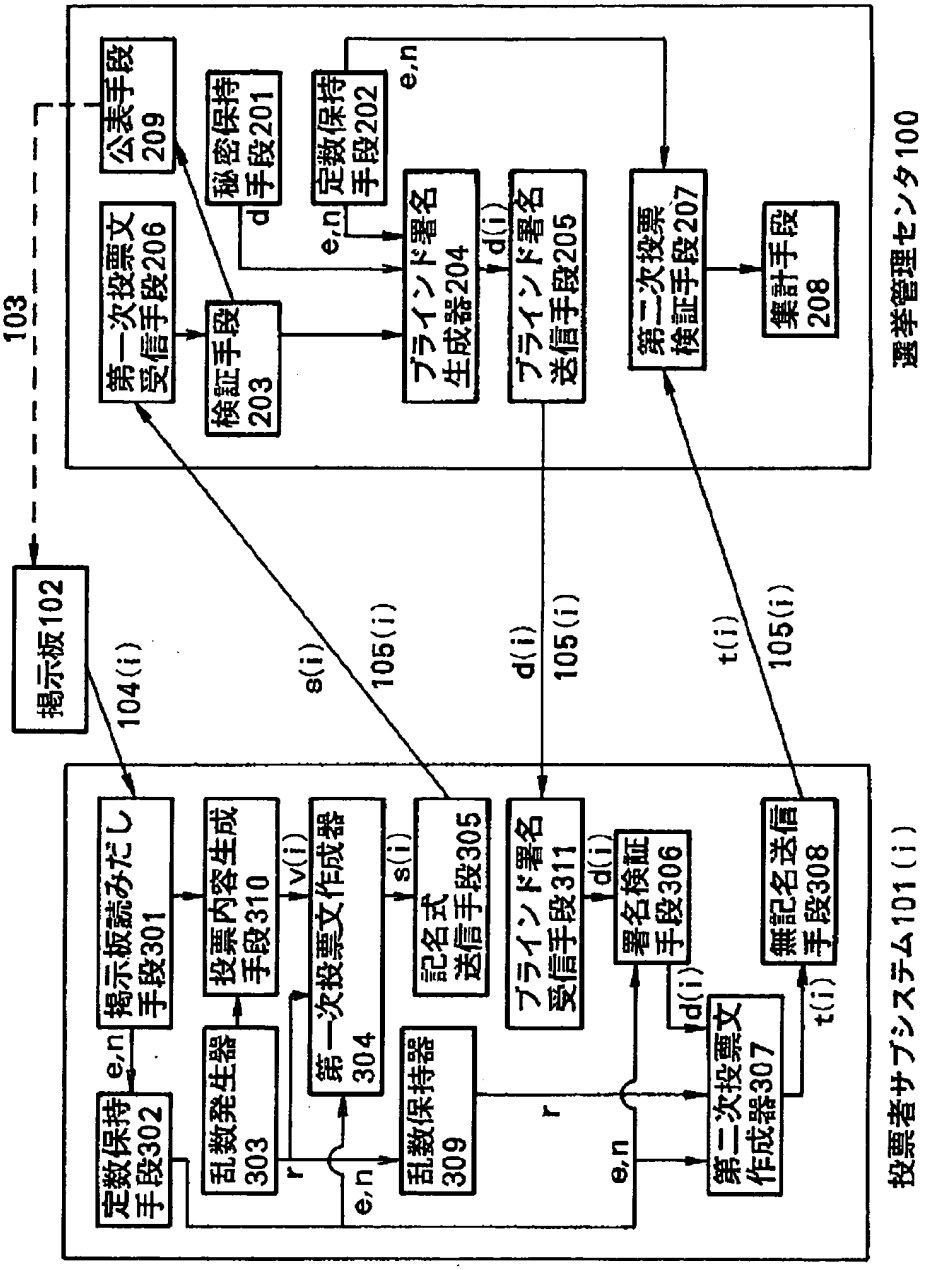
101（i）　投票者サブシステム

102　電子掲示板

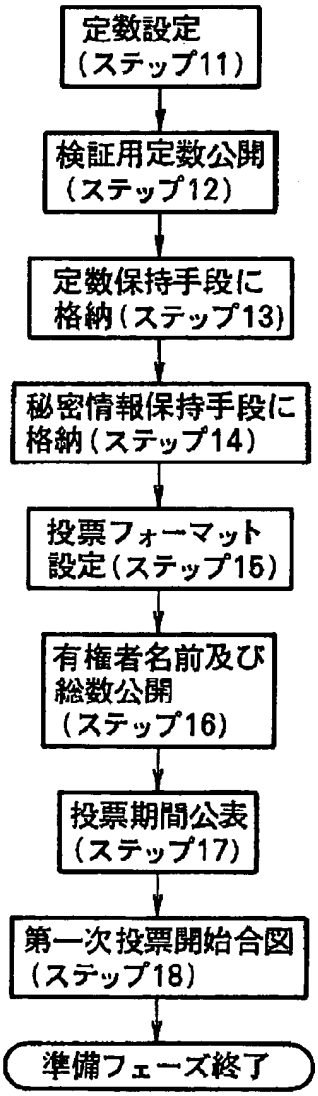
【図2】



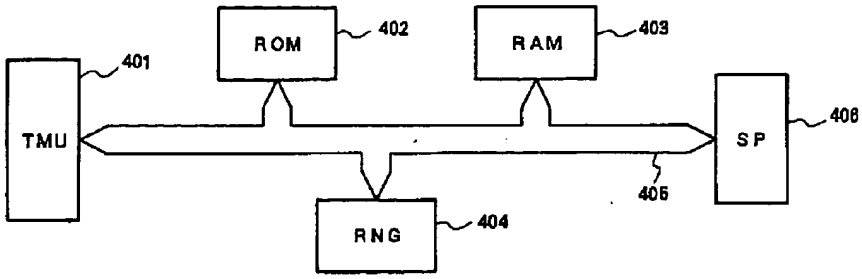
【図1】


選挙管理センタ100
公表手段209
秘密保持手段201
定数保持手段202
第一次投票文受信手段206
検証手段203
ブラインド署名生成器204
ブラインド署名送信手段205
第二次投票検証手段207
集計手段208
103
掲示板102
104(i)
s(i)
105(i)
d(i)
105(i)
t(i)
105(i)
投票者サブシステム101(i)
掲示板読みだし手段301
定数保持手段302
乱数発生器303
投票内容生成手段310
v(i)
第一次投票文作成器304
s(i)
記名式送信手段305
ブラインド署名受信手段311
d(i)
署名検証手段306
d(i)
無記名送信手段308
t(i)
乱数保持器309
第二次投票文作成器307
e,n
r

【図3】


定数設定
(ステップ11)
検証用定数公開
(ステップ12)
定数保持手段に
格納(ステップ13)
秘密情報保持手段に
格納(ステップ14)
投票フォーマット
設定(ステップ15)
有権者名前及び
総数公開
(ステップ16)
投票期間公表
(ステップ17)
第一次投票開始合図
(ステップ18)
準備フェーズ終了

【図4】


TMU
401
ROM
402
RAM
403
SP
406
405
RNG
404